notification, notice, or posting required under this Part would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This paragraph shall be implemented in the same manner as provided under 45 CFR 164.528(a)(2), in the case of a disclosure covered under such section.

§ 318.5 Methods of notice.

(a) *Individual notice.* A vendor of personal health records or PHR related entity that discovers a breach of security shall provide notice of such breach to an individual promptly, as described in § 318.4, and in the following form:

(1) Written notice, by first-class mail to the individual at the last known address of the individual, or by email, if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice. If the individual is deceased, the vendor of personal health records or PHR related entity that discovered the breach must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available.

(2) If, after making reasonable efforts to contact all individuals to whom notice is required under § 318.3(a), through the means provided in paragraph (a)(1) of this section, the vendor of personal health records or PHR related entity finds that contact information for ten or more individuals is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the breach, in the following form:

(i) Through a conspicuous posting for a period of 90 days on the home page of its Web site; or

(ii) In major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn whether or not the individual's unsecured PHR identifiable health information may be included in the breach.

(3) In any case deemed by the vendor of personal health records or PHR related entity to require urgency because of possible imminent misuse of unsecured PHR identifiable health information, that entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (a)(1) of this section.

(b) *Notice to media.* A vendor of personal health records or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(c) *Notice to FTC.* Vendors of personal health records and PHR related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, then such notice shall be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach. If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach, and submit such a log annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year. All notices pursuant to this paragraph shall be provided according to instructions at the Federal Trade Commission's Web site.

§ 318.6 Content of notice.

Regardless of the method by which notice is provided to individuals under § 318.5 of this part, notice of a breach of security shall be in plain language and include, to the extent possible, the following:

(a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);

(c) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the entity that suffered the breach is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and

(e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

§ 318.7 Enforcement.

A violation of this part shall be treated as an unfair or deceptive act or practice in violation of a regulation under §18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

§ 318.8 Effective date.

This part shall apply to breaches of security that are discovered on or after September 24, 2009.

§ 318.9 Sunset.

If new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered by this part, the provisions of this part shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.